UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/559,725	12/07/2005	Yuichi Futa	2005_1849A	1837

52349 7590 09/30/2008

WENDEROTH, LIND & PONACK L.L.P.
2033 K. STREET, NW
SUITE 800
WASHINGTON, DC 20006

EXAMINER	
KING, JOHN B	

ART UNIT	PAPER NUMBER
4148	

MAIL DATE	DELIVERY MODE
09/30/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/559,725	FUTA ET AL.	
	Examiner	Art Unit	
	JOHN B. KING	4148	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 December 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *See Continuation Sheet*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :5 January 2006 and 7 December 2005.

DETAILED ACTION

1. The instant application having Application No. 10559725 filed on December 7, 2005 is presented for examination by the examiner.

Oath/Declaration

2. The applicant's oath/declaration has been reviewed by the examiner and is found to conform to the requirements prescribed in **37 C.F.R. 1.63.**

Priority

3. As required by **M.P.E.P. 201.14(c)**, acknowledgement is made of applicant's claim for priority based on applications filed on June 12, 2003 (JAPAN 2003-167374).

Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Drawings

4. The applicant's drawings submitted are acceptable for examination purposes.

Specification

5. The disclosure is objected to because it contains an embedded hyperlink and/or other form of browser-executable code. Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. See MPEP § 608.01. **For example, See page 3 of the disclosure.**

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. **Claim 7** recites the limitation **"the encryption transmission apparatus"** on line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9. Claims 1-16 are rejected under 35 U.S.C. 102(b) as being anticipated by Yamamichi et al. (US 2002/0116612 A1) published August 22, 2002, hereinafter referred to as Yamamichi.

As per **claim 1**, Yamamichi discloses an encryption communication system for secret message communication, comprising an encryption transmission apparatus and an encryption reception apparatus **(paragraph 27, Yamamichi teaches having a transmission apparatus and reception apparatus in order to encrypt data.)**, wherein the encryption transmission apparatus includes: a storage unit **[plaintext storage]** that stores therein one message **(paragraph 56, Yamamichi teaches having plaintext storage to store the message to be encrypted.)**; an encryption unit

operable to perform an encryption computation on the message a plural number of times **[multiple ciphertexts] (paragraphs 71 and 77, Yamamichi teaches an encryption unit to perform encryptions. In paragraph 11, Yamamichi also discloses generating n ciphertexts based upon n encryptions by n random numbers.)**, thereby generating ciphertexts equal in number **[n]** to the number of times of the encryption computation **(paragraph 11, Yamamichi discloses the generating of n ciphertexts.)**; a computation unit **[one-way operation unit]** operable to perform a one-way operation on the message, thereby generating a comparison computation **[hash]** value **(paragraphs 67-69, Yamamichi discloses the one-way operation unit which performs a one-way operation (hash) on the data to calculate a value.)**; and a transmission **[transmitting]** unit operable to transmit the ciphertexts and the comparison computation value **(paragraph 81, Yamamichi teaches the transmitting unit transferring the ciphertexts and the hash value.)**, and the encryption reception apparatus includes: a reception **[receiving]** unit operable to receive the ciphertexts and the comparison computation value **(paragraph 84, Yamamichi teaches having the receiving unit receive the ciphertext and the hash value.)**; a decryption **[decrypting]** unit operable to perform a decryption computation, which corresponds to the encryption computation, on each of the ciphertexts **[multiple ciphertexts]**, thereby generating decrypted messages equal in number to the number of the ciphertexts **(paragraph 90, Yamamichi teaches the decrypting unit performing a decryption which is the inverse of the encryption that was used. In paragraph 14, Yamamichi also discloses decrypting multiple ciphertexts.)**; a computation **[one-way**

operation] unit operable to perform the one-way operation on each of the decrypted messages, thereby generating decryption computation **[functional]** values equal in number to the number of the decrypted messages **(paragraphs 97-98, Yamamichi teaches the one-way operation unit performing a one-way operation (hash) on the decrypted information and generating a functional value.)**; and a judging unit operable to compare the decryption computation values with the received comparison computation value, and i) if at least one of the decryption computation values matches the received comparison computation value, output a corresponding decrypted message as a correct decrypted text, and ii) if none of the decryption computation values matches the received comparison computation value, output a decryption error **(paragraphs 119-122, Yamamichi teaches a comparison unit that compares the decryption values and the received values and outputs a particular value if there is a decryption error.)**

As per **claim 2**, Yamamichi discloses the encryption communication system of claim 1 **[See rejection to claim 1 above]**, wherein the encryption computation used by the encryption unit conforms to NTRU cryptosystem **(paragraph 77, Yamamichi teaches using the NTRU encryption cryptosystem to encrypt the data.)**, and the decryption computation used by the decryption unit conforms to the NTRU cryptosystem **(paragraph 90, Yamamichi teaches decrypting using the inverse of the encryption algorithm which would have to be the NTRU decryption cryptosystem.)**

As per **claim 3**, Yamamichi discloses an encryption transmission apparatus for secret message communication **(paragraph 27, Yamamichi teaches having a**

transmission apparatus and reception apparatus in order to encrypt data.), comprising: a storage unit **[plaintext storage]** that stores therein one message **(paragraph 56, Yamamichi teaches having plaintext storage to store the message to be encrypted.)**; an encryption unit operable to perform an encryption computation on the message a plural number of times **[multiple ciphertexts]**, thereby generating ciphertexts equal in number to the number of times of the encryption computation **(paragraphs 71 and 77, Yamamichi teaches an encryption unit to perform encryptions. In paragraph 11, Yamamichi also discloses generating n ciphertexts based upon n encryptions by n random numbers.)**; a computation unit **[one-way operation unit]** operable to perform a one-way operation on the message, thereby generating a comparison computation value **(paragraphs 67-69, Yamamichi discloses the one-way operation unit which performs a one-way operation (hash) on the data to calculate a value.)**; and a transmission **[transmitting]** unit operable to transmit the ciphertexts and the comparison computation value **(paragraph 81, Yamamichi teaches the transmitting unit transferring the ciphertexts and the hash value.)**

As per **claim 4**, Yamamichi discloses the encryption transmission apparatus of claim 3 **[See rejection to claim 3 above]**, wherein the encryption unit comprises: an encryption computation subunit operable to perform an invertible data conversion on the message thereby generating a converted message, and perform an encryption algorithm on the converted message thereby generating a ciphertext **(paragraphs 71-79, Yamamichi teaches the function of the encrypting unit. Yamamichi teaches generating a random number and using that generated random number along**

with a key to encrypt data. Yamamichi also teaches adding the random number to the data, which is invertible, and then encrypting the data.); and a repetition control subunit operable to control the encryption computation subunit to repeat the generation of converted message and the generation of ciphertext, the plural number of times **(paragraph 11, Yamamichi teaches the generating of multiple ciphertexts.)**

As per **claim 5**, Yamamichi discloses the encryption transmission apparatus of claim 4 **[See rejection to claim 4 above]**, wherein the encryption computation subunit generates a random number of fixed length, and generates the converted message by adding the random number to the message **(paragraphs 70-79, Yamamichi teaches generating a random number and adding that number, to the data to be encrypted, by the information adding unit.)**

As per **claim 6**, Yamamichi discloses the encryption transmission apparatus of claim 5 **[See rejection to claim 5 above]**, wherein the encryption algorithm used by the encryption computation subunit conforms to NTRU cryptosystem **(paragraph 77, Yamamichi teaches the use of the NTRU encryption cryptosystem.)**

As per **claim 7**, Yamamichi discloses an encryption reception apparatus for secret message communication **(paragraph 27, Yamamichi teaches having a transmission apparatus and reception apparatus in order to encrypt data.)**, where the encryption transmission apparatus stores therein one message **(paragraph 56, Yamamichi teaches having plaintext storage to store the message to be encrypted.)**, performs an encryption computation on the message a plural number of times thereby generating ciphertexts equal in number to the number of the encryption

computation **(paragraphs 71 and 77, Yamamichi teaches an encryption unit to perform encryptions. In paragraph 11, Yamamichi also discloses generating n ciphertexts based upon n encryptions by n random numbers.)**, performs a one-way operation on the message thereby generating a comparison computation **[hash]** value **(paragraphs 67-69, Yamamichi discloses the one-way operation unit which performs a one-way operation (hash) on the data to calculate a value.)**, and transmits the ciphertexts and the comparison computation **[hash]** value **(paragraph 81, Yamamichi teaches the transmitting unit transferring the ciphertexts and the hash value.)**, the encryption reception apparatus comprising: a reception unit operable to receive the ciphertexts and the comparison computation **[hash]** value **(paragraph 84, Yamamichi teaches having the receiving unit receive the ciphertext and the hash value.)**; a decryption **[decrypting]** unit operable to perform a decryption computation, which corresponds to the encryption computation, on each of the ciphertexts, thereby generating decrypted messages equal in number to the number of the ciphertexts [**multiple ciphertexts] (paragraph 90, Yamamichi teaches the decrypting unit performing a decryption which is the inverse of the encryption that was used. In paragraph 14, Yamamichi also discloses decrypting multiple ciphertexts.)**; a computation **[one-way operation]** unit operable to perform the one-way operation on each of the decrypted messages, thereby generating decryption computation **[functional]** values equal in number to the number of the decrypted messages **(paragraphs 97-98, Yamamichi teaches the one-way operation unit performing a one-way operation (hash) on the decrypted information and generating a**

functional value.); and a judging unit operable to compare the decryption computation values with the received comparison computation value, and i) if at least one of the decryption computation values matches the received comparison computation value, output a corresponding decrypted message as a correct decrypted text, and ii) if none of the decryption computation values matches the received comparison computation value, output a decryption error **(paragraphs 119-122, Yamamichi teaches a comparison unit that compares the decryption values and the received values and outputs a particular value if there is a decryption error.)**

As per **claim 8**, Yamamichi discloses the encryption reception apparatus of claim 7 **[See rejection to claim 7 above]**, wherein the encryption transmission apparatus performs an invertible data conversion on the message thereby generating a converted message, performs an encryption algorithm on the converted message thereby generating a ciphertext **(paragraphs 70-79, Yamamichi teaches the function of the encrypting unit. Yamamichi teaches generating a random number and using that generated random number along with a key to encrypt data. Yamamichi also teaches adding the random number to the data, which is invertible, and then encrypting the data.)**, and repeats the generation of converted message and the generation of ciphertext, the plural number of times **(paragraph 11, Yamamichi also teaches generating multiple ciphertexts.)**, and wherein the decryption **[decrypting]** unit comprises: a decryption computation subunit operable to perform a decryption algorithm, which corresponds to the encryption algorithm, on a ciphertext thereby generating a decrypted text **(paragraph 90, Yamamichi teaches the decrypting unit**

performing a decryption which is the inverse of the encryption that was used. In paragraph 14, Yamamichi also discloses decrypting multiple ciphertexts.), and perform an inverse conversion of the invertible data conversion on the decrypted text thereby generating a decrypted message **(paragraph 95, Yamamichi discloses the information removing unit removing the random number from the decrypted data, which is the inverse of adding the random number that the encrypting unit performs.)**; and a repetition control subunit operable to control the decryption computation subunit to repeat the generation of decrypted content and the generation of decrypted message, the plural number of times **(paragraph 14, Yamamichi teaches the decrypting of the multiple ciphertexts.)**

As per **claim 9**, Yamamichi discloses the encryption reception apparatus of claim 8 **[See rejection to claim 8 above]**, wherein the encryption transmission apparatus generates a random number of fixed length, and generates the converted message by adding the random number to the message **(paragraphs 70-79, Yamamichi teaches the transmission apparatus generating a random number and adding that number, to the data to be encrypted, by the information adding unit.)**, and wherein the decryption computation subunit generates the decrypted message by removing the random number of fixed length from the decrypted content **(paragraph 95, Yamamichi teaches the reception apparatus having the information removing unit remove the random number from the decrypted content.)**

As per **claim 10**, Yamamichi discloses the encryption reception apparatus of claim 9 **[See rejection to claim 9 above]**, wherein the encryption algorithm used by the

encryption transmission apparatus conforms to NTRU cryptosystem **(paragraph 77, Yamamichi teaches the use of the NTRU encryption cryptosystem.)**, and wherein the decryption algorithm used by the decryption computation subunit conforms to the NTRU cryptosystem **(paragraph 90, Yamamichi teaches decrypting using the inverse of the encryption algorithm which would have to be the NTRU decryption cryptosystem.)**

As per **claim 11**, Yamamichi discloses an encryption transmission method used in an encryption transmission apparatus that stores therein one message and transmits the message in secrecy **(paragraph 58, Yamamichi teaches having storage to store a plaintext message. In paragraph 81, Yamamichi also discloses the transmission apparatus having a transmitting unit to transmit the data.)**, the encryption transmission method comprising: an encryption step of performing an encryption computation on the message a plural number of times, thereby generating ciphertexts equal in number to the number of times of the encrypted computation **(paragraphs 71 and 77, Yamamichi teaches an encryption unit to perform encryptions. In paragraph 11, Yamamichi also discloses generating n ciphertexts based upon n encryptions by n random numbers.)**; a computation step of performing a one-way operation on the message, thereby generating a comparison computation **[hash]** value **(paragraphs 67-69, Yamamichi discloses the one-way operation unit which performs a one-way operation (hash) on the data to calculate a value.)**; and a transmission step of transmitting the ciphertexts and the comparison computation value

(paragraphs 81, Yamamichi teaches the transmitting unit transmitting the data and the hash value to the receiving apparatus.)

As per **claim 12**, Yamamichi discloses an encryption transmission program used in an encryption transmission apparatus that stores therein one message and transmits the message in secrecy **(paragraph 58, Yamamichi teaches having storage to store a plaintext message. In paragraph 81, Yamamichi also discloses the transmission apparatus having a transmitting unit to transmit the data. In paragraph 56, Yamamichi also teaches an encryption program.)**, the encryption transmission program comprising: an encryption step of performing an encryption computation on the message a plural number of times, thereby generating ciphertexts equal in number to the number of times of the encrypted computation **(paragraphs 71 and 77, Yamamichi teaches performing encryptions. In paragraph 11, Yamamichi also discloses generating n ciphertexts based upon n encryptions by n random numbers.)**; a computation step of performing a one-way operation on the message, thereby generating a comparison computation **[hash]** value **(paragraphs 67-69, Yamamichi discloses the one-way operation unit which performs a one-way operation (hash) on the data to calculate a value.)**; and a transmission step of transmitting the ciphertexts and the comparison computation value **(paragraphs 81, Yamamichi teaches the transmitting unit transmitting the data and the hash value to the receiving apparatus.)**

As per **claim 13**, Yamamichi discloses the encryption transmission program of claim 12 **[See rejection to claim 12 above]**, being recorded in a computer-readable

recording medium **(paragraphs 260-264, Yamamichi teaches the computer program being stored in a computer readable medium.)**

As per **claim 14**, Yamamichi discloses an encryption reception method used in an encryption reception apparatus that receives a message from an encryption transmission apparatus in secrecy **(paragraph 84, Yamamichi teaches the receiving unit receiving the encrypted data from the transmission unit.)**, where the encryption transmission apparatus stores the message therein **(paragraph 58, Yamamichi teaches the transmission apparatus having a plaintext storage to store the message to be encrypted.)**, performs an encryption computation on the message a plural number of times thereby generating ciphertexts equal in number to the number of times of the encryption computation **(paragraphs 71 and 77, Yamamichi teaches an encryption unit to perform encryptions. In paragraph 11, Yamamichi also discloses generating n ciphertexts based upon n encryptions by n random numbers.)**, performs a one-way operation on the message thereby generating a comparison computation **[hash]** value **(paragraphs 67-69, Yamamichi discloses the one-way operation unit which performs a one-way operation (hash) on the data to calculate a value.)**, and transmits the ciphertexts and the comparison computation value **(paragraph 81, Yamamichi teaches a transmitting unit to transmit the data.)**, the encryption reception method comprising: a reception step of receiving the ciphertexts and the comparison computation value **(paragraph 84, Yamamichi teaches the receiving unit receiving the encrypted data and the hash value from the transmission apparatus.)**; a decryption step of performing a decryption

computation, which corresponds to the encryption computation, on each of the ciphertexts, thereby generating decrypted messages equal in number to the number of the ciphertexts **(paragraph 90, Yamamichi teaches the decrypting unit performing a decryption which is the inverse of the encryption that was used. In paragraph 14, Yamamichi also discloses decrypting multiple ciphertexts.)**; a computation step of performing the one-way operation on each of the decrypted messages, thereby generating decryption computation **[functional]** values equal in number to the number of the decrypted messages **(paragraphs 96-98, Yamamichi teaches performing a one-way operation on the decrypted messages to generate a functional value.)**; and a judging step of comparing the decryption computation values with the received comparison computation value, and i) if at least one of the decryption computation values matches the received comparison computation value, outputting a corresponding decrypted message as a correct decrypted text, and ii) if none of the decryption computation values matches the received comparison computation value, outputting a decryption error **(paragraphs 119-122, Yamamichi teaches a comparison unit that compares the decryption values and the received values and outputs a particular value if there is a decryption error.)**

As per **claim 15**, Yamamichi discloses an encryption reception program used in an encryption reception apparatus that receives a message from an encryption transmission apparatus in secrecy **(paragraph 84, Yamamichi teaches the receiving unit receiving the encrypted data from the transmission unit.)**, where the encryption transmission apparatus stores the message therein **(paragraph 58,**

Yamamichi teaches the transmission apparatus having a plaintext storage to store the message to be encrypted.), performs an encryption computation on the message a plural number of times thereby generating ciphertexts equal in number to the number of times of the encryption computation **(paragraphs 71 and 77, Yamamichi teaches an encryption unit to perform encryptions. In paragraph 11, Yamamichi also discloses generating n ciphertexts based upon n encryptions by n random numbers.)**, performs a one-way operation on the message thereby generating a comparison computation **[hash]** value **(paragraphs 67-69, Yamamichi discloses the one-way operation unit which performs a one-way operation (hash) on the data to calculate a value.)**, and transmits the ciphertexts and the comparison computation value **(paragraph 81, Yamamichi teaches the transmitting unit transmitting the data and one-way operation value (hash value) to the receiving apparatus.)**, the encryption reception program comprising: a reception step of receiving the ciphertexts and the comparison computation value **(paragraph 84, Yamamichi teaches the receiving unit receiving the encrypted data and the hash value from the transmission apparatus.)**; a decryption step of performing a decryption computation, which corresponds to the encryption computation, on each of the ciphertexts, thereby generating decrypted messages equal in number to the number of the ciphertexts **(paragraph 90, Yamamichi teaches the decrypting unit performing a decryption which is the inverse of the encryption that was used. In paragraph 14, Yamamichi also discloses decrypting multiple ciphertexts.)**; a computation step of performing the one-way operation on each of the decrypted messages, thereby generating

decryption computation **[functional]** values equal in number to the number of the decrypted messages **(paragraphs 96-98, Yamamichi teaches performing a one-way operation on the decrypted messages to generate a functional value.)**; and a judging step of comparing the decryption computation values with the received comparison computation value, and **i)** if at least one of the decryption computation values matches the received comparison computation value, outputting a corresponding decrypted message as a correct decrypted text, and **ii)** if none of the decryption computation values matches the received comparison computation value, outputting a decryption error **(paragraphs 119-122, Yamamichi teaches a comparison unit that compares the decryption values and the received values and outputs a particular value if there is a decryption error.)**

As per **claim 16**, Yamamichi discloses the encryption reception program of claim 15 **[See rejection to claim 15 above]**, being recorded in a computer-readable recording medium **(paragraphs 260-264, Yamamichi teaches the computer program being stored in a computer readable medium.)**

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JOHN B. KING whose telephone number is (571)270-7310. The examiner can normally be reached on Mon. - Thur. 7:30 AM - 5:00 PM est..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Thomas Pham can be reached on (571)272-3689. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JBK

/THOMAS K PHAM/
Supervisory Patent Examiner, Art Unit 4148